EXHIBIT K

Real-time attack recognition and response:

A solution for tightening network security

INTERNET SECURITY SYSTEMS
41 Perimeter Center
Suite 660
Atlanta, GA 30346
(800) 776-2362
www.iss.net

Table of Contents

Executive summary 1

Networks are more vulnerable to attack 2

The Internet increases vulnerability 2

Security must be enhanced 2

Closing the gap 4

Attack detection 4

Attack response 5

Combining software tools to enhance security 5

Requirements for effective attack recognition and response 5

The RealSecure solution 6

Advanced architecture 7

Recognition engine 7

Response Engine 8

Administrator's Module 9

Manual response 10

Easy configuration 11

Meaningful reports 11

Conclusions 12

About Internet Security Systems, Inc. 13

Executive summary

Enterprise networks are becoming more difficult to secure for several important reasons. As organizations connect their local area networks (LANs) into wide area enterprise networks, these networks become more complex and, therefore, more difficult to secure. In an effort to share information and streamline operations, organizations are also opening their networks to business partners, suppliers, and other outsiders. These open networks are more susceptible to attack than their predecessors. In addition, organizations are connecting their internal networks to the Internet to reap the benefits of its assorted services and nearly universal reach. Connecting to the Internet exposes internal networks to millions of outsiders and greatly increases the difficulty of maintaining effective security.

Technology vendors are responding with a variety of security solutions to help organizations protect their internal networks from outside attacks. These solutions include firewalls, operating system security mechanisms such as authentication and access privilege levels, and encryption. Even with this combination of security solutions in place, hackers still manage to penetrate. Complicating the problem of maintaining effective security is the fact that networks are continually changing to meet shifting business situations, such as reorganizations, acquisitions, and mergers.

What is required is a security solution that is independent of conventional security mechanisms—one that detects and intercepts security breaches that penetrate the network's first line of defense. One such solution is an *attack recognition and response system*.

Typically implemented in software, an attack recognition and response system continually monitors network traffic, looking for known patterns of attack. When it detects an unauthorized activity, the software responds automatically with predetermined actions. It may report the attack, log the event, or terminate the unauthorized connection. Attack recognition and response software operates in concert with other security mechanisms to provide truly effective security.

This paper presents the concepts of network monitoring, attack recognition and response software. It describes the need for additional network security, and explains how attack recognition and response software addresses this need. It also examines the requirements for an effective attack recognition and response system. Finally, it describes RealSecure, a real-time attack recognition and response system that meets these requirements.

Networks are more vulnerable to attack

Organizations are continuing to expand their enterprise networks—connecting and consolidating local area networks into wide area networks (WANs). The resulting increase in complexity makes security more difficult and increases the vulnerability of the network to attack by both external and internal users. In addition, organizations are continuing to open their networks to outsiders. An example of this would be interconnecting enterprise networks with those of outside organizations. This further increases vulnerability to attack.

The Internet increases vulnerability

Today, many organizations are connecting their internal networks to the Internet to meet important business objectives that include:

- *Giving employees access to Internet resources.* Employees can increase their productivity by taking advantage of the vast amount of information and services on the Internet.
- *Giving external users access to the internal network from the Internet.* Organizations need to make internal network information available to users in the outside world, including customers, suppliers, and business partners.
- *Using the Internet as a basis for commerce.* One of the major attractions of the Internet is that it enables organizations to reach customers in much greater numbers and in far more locations than with conventional commerce vehicles.
- *Using the Internet as wide area network backbone.* The Internet provides an economical medium for connecting local area networks into WANs.

While connecting to the Internet offers numerous advantages, it also exposes internal networks to millions of outsiders. This exposure intensifies the need for comprehensive security.

Security must be enhanced

Increasing network complexity, greater openness, and the growing emphasis on the Internet are causing organizations to feel more and more insecure about their networks—and rightly so. These three trends are resulting in significantly higher exposure to both internal and external attacks. Ernst & Young/ Information Week's fourth annual Information Security Survey from 10/21/96 reveals some eye-opening statistics:

> "78% of Information Security chiefs, Information Security Officers and other high-level executives lost money from security breeches. More than 25% reported losses greater than twenty-five thousand dollars, and inside hackers were at fault for nearly 32%. With these breeches in security and serious financial losses, 70% have no more than three people dedicated to corporate security."

A variety of security devices are being deployed to protect internal networks from outside attacks. One type of security device receiving a considerable amount of attention today is the firewall. A firewall is typically implemented in software. It interposes a barrier at the point of connection between the Internet and the corporate internal network to keep out attackers. A recent survey in InfoWeek showed that 20 percent of respondents already have a firewall and over 40 percent more plan to implement one.

Firewalls, however, are not foolproof. They are difficult to configure, even by experts. They require the accurate configuration of numerous and confusing access control lists. Even a minor error in entering configuration information can result in a gaping hole in security. Complicating the issue is that firewall configurations must be continually updated to allow access to new network services required by end-users and to keep up with changing security policies. These policy changes are driven by changing business situations, such as reorganizations, mergers, and acquisitions. As a result of the complexity and continual change of firewall configurations, administrators are apt to miss potential security holes.

Networks provide an ideal medium to encourage collaboration among people. As a result, organizations are demanding network software that allows an increasing richness of collaboration and interaction among people. Of course, implied in this demand is that security not be compromised by increased levels of collaboration. As a result, configuring firewalls will become even more difficult as organizations increase their level of interaction with partners, suppliers, and customers.

Even properly configured firewalls have known weak spots. Using techniques such as IP spoofing and IP fragmentation, hackers have demonstrated the ability to pass through a large percentage of the firewalls on the market today. Another problem is that, in many situations, hackers can circumvent firewalls entirely. For example, if an internal user connects a modem to a networked PC and forgets to associate a password with the modem line, a hacker could enter the internal network directly through that modem, completely bypassing the firewall. Internal attacks from inside the firewall are also a frequent source of break-ins. In fact, internal attacks, often committed by disgruntled employees or co-opted contractors, account for the majority of network break-ins. FBI reports show that more than 60 percent of computer crimes originate inside the enterprise.

In addition to add-on devices such as firewalls, security mechanisms are also built into operating systems. Operating systems provide user authentication through passwords, and they provide multi-level access control to information. Like firewalls, however, operating system security is also vulnerable to attack. Operating systems are difficult to configure from a security perspective. Another problem is that software updates to operating systems can introduce security holes that are unknown to the administrator. Additionally, access control at the operating system level does not necessarily map directly to the network level. As a result, it isn't always possible for operating system access control to help block attacks from the network.

The rapid increase of network complexity and the attendant increase in the difficulty of securing networks has caused numerous vulnerabilities that far exceed an organization's capacity to deal with them effectively. To make matters worse, new vulnerabilities are being introduced into the networking environment every day. The result is a widening gap between an organization's security policy and its actual security practice. Organizations need solutions that help close this gap by augmenting traditional security systems with enhanced security mechanisms.

Closing the gap

There are two effective methods for augmenting conventional security systems to close the gap between security policy and security practice:

- *Attack recognition and response software.* This software continually monitors network traffic, looking for known patterns of attack. It runs on network machines that are strategically located at control points throughout the network , such as near an Internet router link or near a LAN on which critical data resides. When the software detects unauthorized activity, it responds automatically with some form of defined action. These actions can typically be configured by the administrator. Attack recognition and response software is like a burglar alarm. The alarm detects an intrusion in process and responds automatically by sounding an audible signal or telephoning the police.

- *Security scanning software.* This software probes the network with a series of tests to ferret out potential security vulnerabilities. It produces a detailed report on the weak spots that it finds, with sufficient information to enable corrective action. Security scanning software is similar to a security consultant. The consultant examines the organization's facilities looking for security weak spots and reports on the weaknesses discovered along with the necessary corrective actions to minimize or eliminate them.

This paper focuses on attack recognition and response software.

Attack detection

Attack recognition and response software typically detects attacks using one of the following two approaches:

- *Rule-based.* This approach draws from a library of known attack patterns or unauthorized activity and watches for those specific types of attacks. This is similar to the technique used in virus detection. The attack pattern library is updated continually as new types of attacks are discovered.

- *Statistical anomaly.* This approach operates on the assumption that users and networks always exhibit a predictable pattern of behavior and do not depart from this pattern over short periods of time. A deviation is considered to be an attack.

Attack response

Attack recognition and response software can be configured to react automatically to an attack in a variety of ways. It can:

- Log the event along with associated information.
- Alert appropriate personnel through console messages, e-mail, or pagers.
- Terminate the offending connection.
- Call a user-defined script or program.
- Perform a combination of these actions.

Combining software tools to enhance security

Attack recognition and response software can operate in conjunction with security scanning software to provide more complete protection. For example, a vulnerability may appear temporarily and then disappear between security scans. As a result, the scanning software does not detect it. The attack recognition and response software, however, does detect an attack through that vulnerability. The software reports the attack and logs information about it. The administrator can then analyze the information and implement additional security mechanisms to eliminate or reduce the vulnerability.

In another example, the scanner may identify a particular vulnerability in a network service. The benefit presented by that service, however, may outweigh the security risks it brings about. As a result, the organization may continue to allow that service despite its known vulnerability to attack. The attack recognition and response software can detect an attack through that vulnerability and enable the organization to react before the attack compromises the network.

Requirements for effective attack recognition and response

Attack recognition and response software must meet a number of requirements to provide truly effective protection against attacks. The major requirements include:

- *Real-time operation.* The attack recognition and response software must be capable of detecting, reporting, and reacting to suspected attacks in real time. Software that merely logs events and provides audit logs for examination after-the-fact is ineffective. After-the-fact detection is like a burglar alarm that goes off long after the burglar has fled. In addition, many attackers erase logs during the break-in, so their intrusion cannot be detected by merely scanning an event log.

- *Capable of update.* Just as there is a continual launch of new computer viruses, hackers continually find new ways to break into computer systems. As a result, attack

recognition and response software must be capable of continually adding to its knowledge base of known break-in patterns and unauthorized activity.

- *Run on popular network operating systems.* The software must support existing network infrastructures. That means it must support existing network operating systems, such as UNIX and Windows NT.

- *Easy to configure.* Configuration should be easy, without sacrificing effectiveness. The attack recognition and response software should provide a default configuration so that administrators can deploy it quickly and optimize it over time as information accumulates. In addition, the software should provide sample configurations to guide administrators in setting up the system.

- *Easy to manage.* Rapidly rising network management costs present a significant problem for organizations. Attack recognition and response software must be easy to manage so that it does not contribute to this problem. Management of the software over the network from a central location is essential. In addition, the software should be easy to integrate with the existing network management infrastructure. This requires compliance with network management standards such as SNMP.

- *Adaptable to changing security policies.* Today's business environment is dynamic. Organizations are continually changing, driven by many factors, including reorganizations, mergers, and acquisitions. As a result, security policies are also in flux. To remain effective, attack recognition and response software should be easy to adapt to changing security policies. This ensures that these policies can be implemented in fact as well as on paper.

- *Nonobtrusive.* The software should operate in a nonobtrusive way. That is, it should not degrade network performance. It should be transparent to authorized users so that it does not hamper productivity. In addition, it should not alert the intruder to its presence.

The RealSecure solution

RealSecure, from Internet Security Systems, is a real-time monitoring, attack recognition, and response system. It monitors packet flow over a network in real time and analyzes packets for known attack patterns and unauthorized activity using a rule-based approach. When it detects an attack, it reacts automatically according to its configuration. RealSecure can react in four ways when it detects an attack:

- It can alert appropriate personnel through administrator's console messages, e-mail, or pager alerts.
- It can log the event along with associated information.

- It can kill the event by terminating its connection.
- It can initiate a user-supplied script.

Organizations can strengthen security with RealSecure in three primary ways:

- They can use it as an effective, second line of defense behind firewalls, intercepting and disposing of attacks that get through the firewalls, or that originate inside the firewalls.
- They can use it as a means of measuring the effectiveness of the current network security mechanisms by testing whether they are indeed keeping out what they are supposed to be keeping out. For example, RealSecure can detect when a Telnet session is being established from the Internet although the firewall has been configured to disallow Telnet sessions from the Internet.
- They can use it in conjunction with a security assessment package to provide feedback on risks they have accepted in order to provide access to a service that users need but that makes the network vulnerable to attack. RealSecure can determine the number of attempted break-ins through that vulnerability. If the number of attempted break-ins is high, the organization may change the decision to make that service available.

RealSecure provides useful reports on its findings to help organizations assess and tighten their security.

Advanced architecture

RealSecure consists of three components:

- *Recognition engine.* This component monitors the network in real time, detecting and reporting attacks. It reports events to the Administrator's Module.
- *Response Engine.* This component reacts automatically to recognized attack events, triggering prespecified actions ranging from logging attacks and alerting the administrator to terminating offending connections.
- *Administrator's Module.* This component provides GUI (graphical user interface) management of the Recognition and Response engines. The Administrator's Module can monitor and manage all recognition and response engines from a single GUI, simplifying network management.

Recognition engine

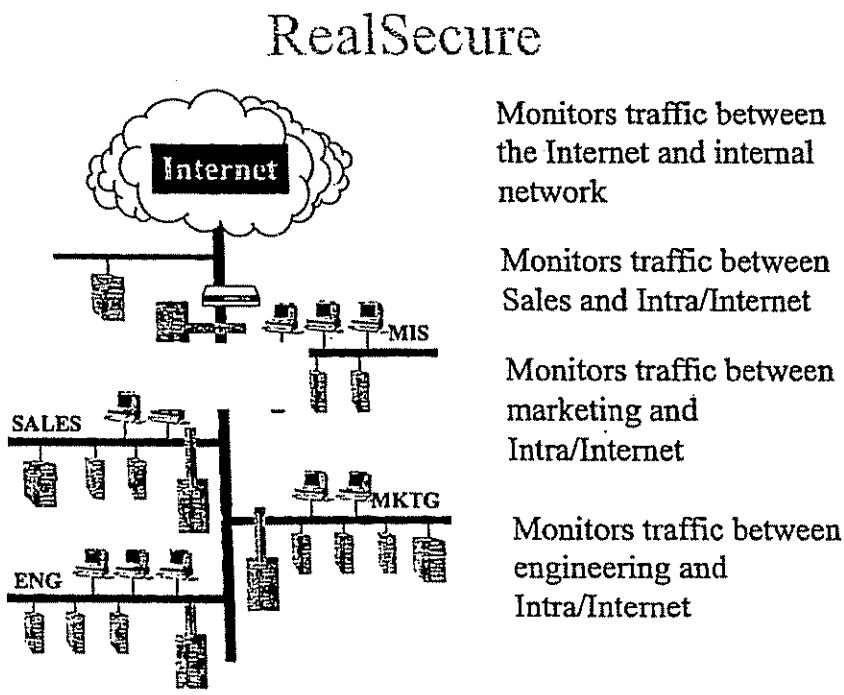
The Recognition engine leverages Internet Security System's in-depth knowledge of how systems are attacked. The Engine can detect low-level IP attacks, such as those using IP spoofing, IP fragmentation, or SYN flooding. These low-level forms of attack can bypass packet filter firewalls. The Engine can also detect high-level attacks, such as from Web, FTP, NFS, NIS, or e-mail sessions.

The administrator can configure the Recognition engine to implement specific security policies. The engine can react to (or ignore) connections based on specific packet types, source, and destination IP addresses or address ranges, port numbers, or particular types

of attack patterns. This flexibility enables the administrator to set up custom monitoring for individual hosts and networks. Because the Recognition engine is a passive monitor, operating like a sniffer with built-in security knowledge, it doesn't degrade network performance.

As Figure 1 shows, an organization can place multiple Recognition engines in strategic locations in its network topology. An organization can also use multiple Recognition engines in parallel at a single location to accommodate high bandwidth connections, such as T3 access to the Internet.

Figure 1
The RealSecure real-time attack recognition and response system



Response Engine

The Response Engine is flexible and can be configured to react automatically to detected attacks in a variety of ways:

- *Alert appropriate people.* The Response Engine can alert the administrator through the Administrator Module, it can send e-mail messages, and it can activate pagers.

- *Log attack.* The Response Engine can be configured to log the attack. It can log the event only or the entire attack session, including all the hacker's keystrokes. The administrator can play back the session later; in its entirety, through an easy-to-use, VCR-like GUI control panel.
- *Terminate session.* The Response Engine can be configured to reset the connection on both the attacker's machine and the target machine when it detects an attack. It terminates the session by sending a reset (RST) packet to the attacker's machine, and it sends an RST packet to the target machine, spoofing the attacker's IP address.
- *Initiate user-supplied scripts.* The response can also be customized with user-supplied scripts that are activated when an attack is detected. In this way, reaction can be tailored to the specific needs of the organization.

The Response Engine's ability to react automatically provides proactive security, without requiring administrator intervention.

Administrator's Module

The Administrator's Module provides a single point of management and control for all Recognition and Response engines in the network. The administrator can configure the Recognition and Response engines from the Administrator's Module. In addition, the Module collects and presents events reported by the Recognition engines in an easy-to-read GUI display.

When a Recognition engine detects an attack, it reports it to the Administrator's Module. The module displays the event in real time, as it is happening, optionally including the hacker's keystrokes and a copy of the hacker's screen. To allow easy, attack events are classified and displayed by high, medium, or low priority. (See Figure 2.)

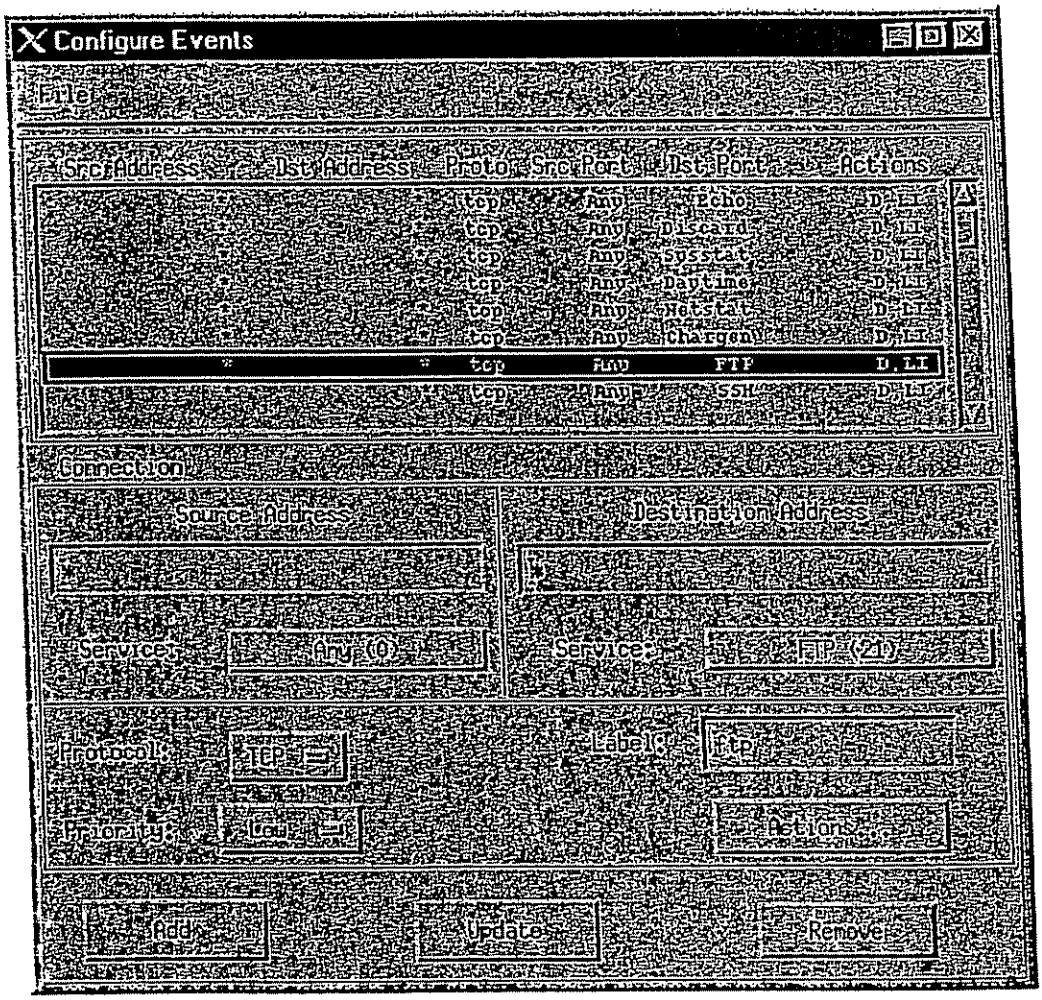


Figure 2
The RealSecure Administrator's Module

Manual response

In addition to automatic response, the administrator can respond manually to reported attacks in a variety of ways using the Administrator's Module GUI:

- *Request additional information.* The administrator can request the Engine to provide more detailed information on the reported attack. This information can include the packet source and packet data, such as e-mail headers.

- *Instruct RealSecure to log the event.* If automatic event logging has not been configured for this event, the administrator can request RealSecure to log the reported event.
- *Instruct RealSecure to kill the event.* If automatic session termination has not been configured for this event, the administrator can request RealSecure to terminate the session.

The administrator can combine automatic and manual response to maintain the exact level of control required.

Easy configuration

The administrator configures RealSecure through the easy-to-use Administrator Module GUI. The configuration specifies the types of checks to be performed by the Recognition Engine and the response to be initiated by the response Engine for each type of attack detected. Through the GUI, the administrator can custom-tailor a security model of the network to match the organization's security policy.

RealSecure includes a default configuration to allow an organization to get up and running quickly. The default configuration is biased towards tight security to ensure the protection of the monitored network. RealSecure also includes a variety of sample configurations at different levels to provide starting configurations for various types of security policies.

Meaningful reports

RealSecure can generate meaningful reports from its event log files. These reports can include such information as the amount of data processed by a Web server each day, or the number of connections that were killed each day and from whom. The Administrator Module can display these reports in graphical form, such as bar or pie charts, for easy review and analysis. (See Figure 3.)

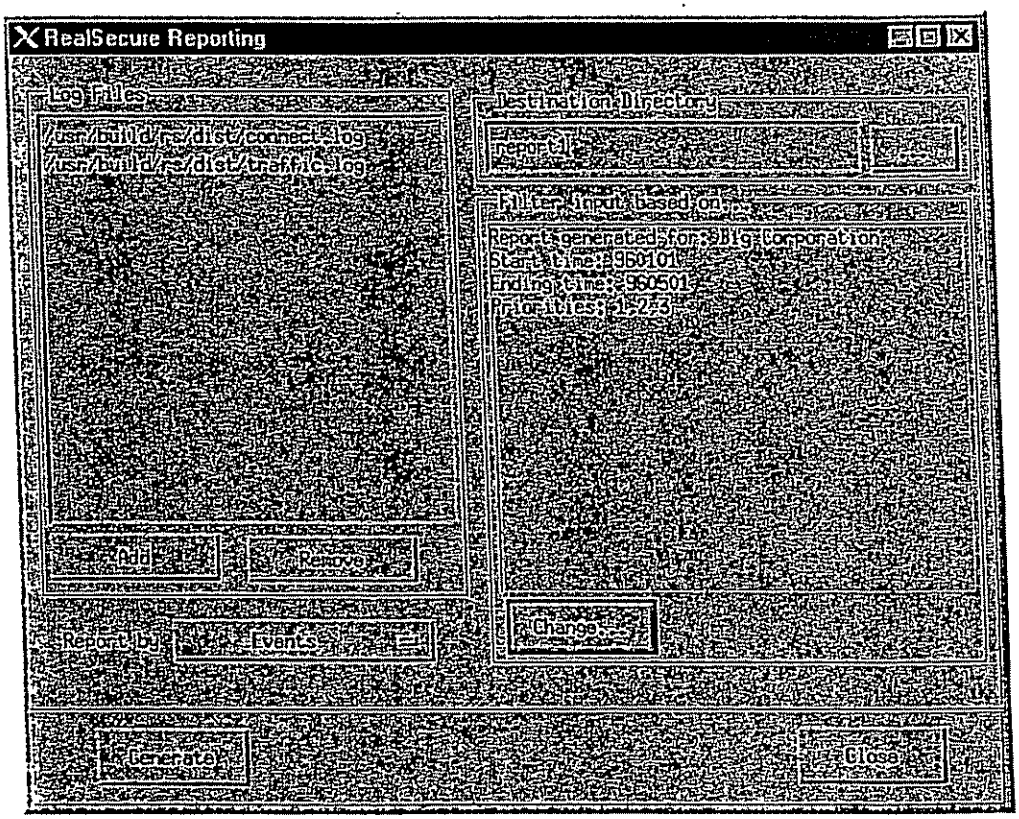


Figure 3
Typical RealSecure Report

Administrators can use these reports to optimize security. The suggested method of implementation is to start with overly tight filtering using the default configuration. The administrator can use the information in the reports to tune the filtering over time as he or she gains better understanding of normal network activity. This iterative tuning reduces the number of alerts without relaxing security.

Conclusions

In order for organizations to compete effectively in today's business environment it is essential that they increase their use of networks, including:

- Expanding the reach of their internal networks by interconnecting LANs into WANs,.
- Opening their internal networks to outside organizations to gain higher levels of interaction with their business partners.

- Taking full advantage of the power of the Internet.

However, the increasing use of networks brings with it increased vulnerability to network break-ins. Traditional network security solutions such as firewalls, operating system security mechanisms, and encryption protect internal networks to a large degree, but hackers still manage to penetrate. Break-ins—whether internal or external—can be costly, and expose sensitive and confidential information to the outside world.

RealSecure augments existing security mechanisms and helps reduce the gap between an organization's security policy and its actual security practice. It enables organizations to measure the effectiveness of their current network security mechanisms in implementing security policy. It also provides an effective second line of defense behind existing mechanisms.

With the combination of RealSecure and traditional security mechanisms, organizations can continue to expand their use of networks, without increasing their risk of network break-ins. In this way, they can maintain their competitive edge while also keeping their security practices in line with their security policies.

About Internet Security Systems, Inc.

Internet Security Systems, Inc. (ISS) is the leading supplier of network security assessment tools, providing comprehensive and innovative audit, monitoring, and response software. The Atlanta-based company's flagship product, Internet Scanner, is the leading commercial attack simulation and security audit tool used to facilitate continuous network security improvement in corporations, financial institutions, and government agencies worldwide. The ISS SAFEsuite family of products provides a comprehensive security framework specifically designed to assess a variety of network security issues confronting web sites, firewalls, servers and workstations. For more information about ISS and its products, contact the company at (770) 395-0150 or visit the ISS web site at http://www.iss.net.